Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for authenticating data and indicating an authentication of the data ~~at a server~~, the method comprising:
   - ~~a.~~ receiving a data request from a client;
   - ~~b.~~ retrieving data based on the data request to obtain retrieved data;
   - ~~c.~~ formatting the retrieved data in real-time at the server to create formatted data, wherein the formatted data includes an authenticity key;
   - ~~d.~~ returning the formatted data to the client;
   - ~~e.~~ facilitating authentication of the authenticity key to verify a source of the formatted data;
   - ~~f.~~ retrieving, at the client, a preferences key from ~~said~~ the server based on ~~said~~ the authentication; and,
   - ~~g.~~ decrypting a preferences file having a authenticity stamp instruction using ~~said~~ the preferences key, wherein the authenticity stamp is at least one of text, graphic, and audio.
2. (original) The method of Claim 1, wherein the formatted data is a web page.
3. (previously presented) The method of Claim 1, further comprising:
   - ~~a.~~ reading the formatted data at the client;
   - ~~b.~~ determining if the formatted data includes the authenticity key; and,
   - ~~c.~~ verifying authenticity based on the authenticity key when the formatted data includes the authenticity key.
4. (previously presented) The method of Claim 3, further comprising displaying the formatted data based on the verification of the authenticity key.
5. (previously presented) The method of Claim 4, wherein an authenticity stamp is displayed for formatted data that has been successfully verified.
6. (previously presented) The method of Claim 4, wherein an authenticity stamp is displayed for a graphical image.
7. (previously presented) The method of Claim 4, wherein a non-authenticity stamp is displayed for formatted data that has not been successfully verified.

8. (currently amended) A system for authenticating data and indicating an authentication of the data, the system comprising:

~~a.~~ a client;

~~b.~~ a server;

~~c.~~ a network, wherein the client and the server communicate via the network; and

~~d.~~ an authentication server, wherein the authentication server is in communication with the server, the authentication server being configured to insert an authenticity key in real time into the data requested from the client, thereby facilitating the client to authenticate the authenticity key to verify the source of the data; and, wherein the client is configured to:

~~e.~~ retrieve a preferences key upon the verification of the source of the data, wherein the preferences key is retrieved from the authentication server and is used to decrypt a preferences file having a visual signature instruction on the client.

9. (previously presented) The system of Claim 8, wherein the client comprises a browser, wherein pages are displayed to a user on a display device on the client.

10. (previously presented) The system of Claim 8, wherein the server sends a page including the authenticity key to the client.

11. (previously presented) The system of Claim 10, wherein the client verifies authenticity of the page based on the authenticity key.

12. (previously presented) The system of Claim 11, wherein the page is displayed on the client, and wherein the display includes an indication of the authenticity of the page.

13. (cancelled).

14. (currently amended) In a computer system for authenticating data and indicating an authentication of the data ~~at a server~~, a computer-readable medium holding computer executable instructions for performing a method comprising the steps of:

~~a.~~ receiving a data request from a client;

~~b.~~ retrieving data based on the data request to obtain retrieved data;

~~c.~~ formatting the retrieved data in real-time at ~~said~~ the server to create formatted data, wherein the formatted data includes an authenticity key;

~~d.~~ returning the formatted data to the client;

~~e.~~ facilitating authentication of the authenticity key to verify a source of the formatted data;

~~f.~~ retrieving, at the client, a preferences key from ~~said~~ the server based on ~~said~~ the authentication; and,

~~g.~~ decrypting a preferences file having a visual signature instruction using the ~~said~~ preferences key.

15. (currently amended) The computer system of Claim 14, wherein ~~said~~ the formatted data is a web page.

16. (previously presented) The computer system of Claim 14, wherein computer executable instructions further comprise the steps of:

~~a.~~ reading the formatted data at the client;

~~b.~~ determining if the formatted data includes the authenticity key; and,

e. verifying authenticity based on the authenticity key when the formatted data includes the authenticity key.

17. (previously presented) The computer system of Claim 16, wherein the computer executable instructions further comprise the step of: displaying the formatted data based on the verification of the authenticity.

18. (previously presented) The computer system of Claim 17, wherein an authenticity stamp is displayed for formatted data that has been successfully verified.

19. (previously presented) The computer system of Claim 17, wherein a non-authenticity stamp is displayed for formatted data that has not been successfully verified.

20. (previously presented) The method of claim 1, wherein the receiving and returning steps are implemented via at least one of an internet, interactive television system, broadband system, regular band system, wireless system, radio transmission, landline phone system, and cellular phone system.

21. (previously presented) The method of claim 1, wherein the step of authenticating the authenticity key to verify the source of the formatted data comprises a browser plug-in interfacing with a MIME type to authenticate a private key included in the formatted data.

22. (currently amended) The system of claim 8, wherein ~~said~~ the authentication server is configured to authenticate a user ID and a password.

23. (currently amended) The system of claim 8, wherein ~~said~~ the authentication server is configured to sign a web page.

24. (currently amended) A method for authenticating data and indicating an authentication of the data ~~at a server~~, the method comprising:
receiving a data request from a client;
retrieving data based on the data request to obtain retrieved data;
determining if ~~said~~ the data includes a code which requires the data to be authenticated;
formatting the retrieved data in real-time at ~~said~~ the server to create formatted data, wherein the formatted data includes an authenticity key;
returning the formatted data to the client;
facilitating authentication of the authenticity key to verify the source of the formatted data; ~~and,~~
retrieving, at the client, a preferences key based on the authentication, wherein the preferences key is retrieved from the ~~server.~~ server; and,
decrypting a preferences file having a visual signature instruction using the preferences key.

25. (currently amended) The method of claim 24, further comprising:
obtaining the visual signature instruction from ~~instructions~~ within the preferences file; and,
inserting a visual signature into the formatted data based on the visual signature instruction ~~instructions~~ stored in the preferences file.

26. (currently amended) The method of claim 24 further comprising:
~~decrypting the preferences key using a master preferences key;~~
obtaining the visual signature instruction from ~~instructions~~ within the preferences file; and,
inserting a visual signature into the formatted data based on the visual signature instruction ~~instructions~~ stored in the preferences file.

27. (currently amended) The method of claim 1, further comprising:
obtaining the visual signature instruction from ~~instructions~~ within the preferences file; and,

inserting a visual signature into the formatted data based on the visual signature instruction ~~instructions~~ stored in the preferences file.

28. (currently amended) The method of claim 1, further comprising:

decrypting the preferences key using a master preferences key;

obtaining the visual signature instruction from ~~instructions~~ within the preferences file; and,

inserting a visual signature into the formatted data based on the instructions stored in the preferences file.

29. (currently amended) A method for authenticating data and indicating an authentication of the data ~~at a server~~, the method comprising:

receiving a data request from a client;

retrieving data based on the data request to obtain retrieved data;

formatting the retrieved data in real-time at the server to create formatted data, wherein the formatted data includes an authenticity key;

returning the formatted data to the client; and,

facilitating authentication of the authenticity key to verify a source of the formatted data;

decrypting a preferences key;

decrypting a preferences file using the preferences key;

obtaining an authenticity stamp instruction from ~~instructions~~ within the preferences file; and,

inserting ~~a visual signature~~ an authenticity stamp into the formatted data based on the authenticity stamp instruction ~~instructions~~ stored in the preferences file, wherein the authenticity stamp is at least one of text, graphic, and audio.

30. (currently amended) A method for authenticating data and indicating an authentication of the data ~~at a server~~, the method comprising:

receiving a data request from a client;

retrieving data based on the data request to obtain retrieved data;

determining if the data includes a code which requires the data to be authenticated;

formatting the retrieved data in real-time at ~~said~~ the server to create formatted data, wherein the formatted data includes an authenticity key;

returning the formatted data to the client;

facilitating authentication of the authenticity key to verify the source of the formatted data;

decrypting a preferences key;

decrypting a preferences file using the preferences key;

obtaining an authenticity stamp instruction from ~~instructions~~ within the preferences file; and,

inserting ~~a visual signature~~ an authenticity stamp into the formatted data based on the authenticity stamp instruction ~~instructions~~ stored in the preferences file, wherein the authenticity stamp is at least one of text, graphic, and audio.